# V3 VirusBlock 2005
# *用户使用说明书*

## 产品注册
用户购买 V3 Virus Block2005 产品后需在网上进行注册，注册后用户将享受到本公司提供的各种服务，如果用户的计算机还没有连接到互联网，也可以通过电话或者传真进行产品注册

[注意]
在安装 V3 VirusBlock 2005 时如果用户不输入产品序列号，产品将自动安装评估版本，而评估版本是无法进行注册的，没有注册的产品只能享受到三十天的升级和其它的各种服务

## 客户服务
购买 V3 VirusBlock 2005 产品并注册的用户在一年之内免费享受到如下服务（产品的主页）

- 升级最新病毒引擎
- 提供专杀工具
- 各种安全设置信息
- 最新危害严重的病毒警报
- 安全相关信息
- 用户帮助及 FAQ
- 其它实用软件

给用户提供的最新病毒引擎的升级服务是一周进行一次以上，注册用户每周都能收到升级服务的邮件。每周更新最新的病毒引擎能有效的保护用户的计算机，并保证用户的计算机不会受到病毒的感染。如果正在扩散最新危害严重的病毒时，会及时推出针对此类病毒的专杀工具。任何用户都可以从北京安博士信息安全技术有限公司主页(http://www.ahn.com.cn)的[客户服务]菜单上下载专杀工具使用

## 产品的注册及更新
注册产品一年后，如果想继续享受本公司提供的客户服务，就需要重新注册产品，此时用户应付相应的注册费用。产品使用一年后没有重新注册的用户将无法继续享受到最新病毒引擎的升级及其它相关服务，为了让计算机免受病毒的感染，应及时重新注册产品，重新注册产品的详细信息咨询请登陆到北京安博士信息安全技术有限公司主页(http://www.ahn.com.cn)的[客户服务>重新注册（更新用户信息）]菜单

参考
V3 VirusBlock 2005 产品的注册截止日期可以登陆到北京安博士信息安全技术有限公司主页(http://www.ahn.com.cn)的[客户服务>产品注册及确认]菜单上确认

## 客户服务联系方式
如对 V3 VirusBlock 2005 产品的使用方法及重新注册方式有疑问，请用以下联系方式联系我们

| 北京安博士信息安全技术有限公司的客户服务中心 | |
|---|---|
| 地址 | 北京市海淀区中关村东路 18 号财智大厦 C 座 2005 室北京安博士信息安全技术有限公司，邮编：10083 |
| 主页 | http://www.ahn.com.cn |
| E-mail | support@ahn.com.cn<br>V3SOS@ahn.com.cn |
| 电话 | 010-8260-0932（前台）<br>800-8100607（技术支持） |
| 传真 | 010-6219-6003 |



## 1.1. 系统要求

### 用户系统

安装 V3 VirusBlock 2005 产品对计算机配置的要求如下，安装本产品之前请用户确认计算机的配置情况

| 系统配置 | 推荐配置 | 最低配置 |
|---|---|---|
| OS | Windows 98/ME/NT 4.0 Workstation Service Pack 6/2000 Professional/XP | Windows 98 以上 |
| CPU | Pentium III 以上 | Pentium 133MHz 以上 |
| Memory | 256MB | 32MB |
| HDD | 200MB 以上 | 80MB 以上 |
| Resolution | 1024 * 768 | 800 * 600 |
| CD-ROM | 24 倍速以上 | 4 倍速以上 |

[注意]
安装 V3 VirusBlock 2005 产品时需用系统管理员身份登陆，如果用户的计算机系统没有用系统管理员身份登陆将无法安装 V3 VirusBlock 2005 产品

### 邮件客户端程序

如果安装了以下的邮件客户端程序本产品就会对其进行 POP3, Outlook 的监控

- Outlook Express 5.5x 以上
- Netscape 4.x/6.x/7.x
- Eudora 5.2
- Becky 2.0

### 聊天客户端程序

如果安装了以下的聊天客户端程序本产品就会对其进行的监控

- AIM(AOL Instance Messenger) : 5.1.3036 以上
- Yahoo Messenger : 5.5.0.1246 以上
- MSN Messenger : 4.x 以上

# 1.2. 安装

1.　　把 V3 VirusBlock 2005 产品的安装光盘放入光驱里
→ 此时会出现〈正在进行安装…〉的魔法师窗口

参考
如果没有出现 V3 VirusBlock 2005 InstallShield 的魔法师窗口时采用以下的方法进行安装
1. 点击“**状态栏**”→**开始**→**运行**
在弹出的“**运行**”窗口里输入产品的光盘盘符及产品的安装文件名称后点击“**确认**”按钮（例：‘D:\install.exe’）

2.　　结束安装准备后会出现 V3 VirusBlock 2005 InstallShield 的魔法师窗口，点击“**下一步**”按钮后继续执行下一步的安装步骤

3.　出现<用户协议>窗口。 阅读 V3 VirusBlock 2005 的用户授权协议后，如果同意协议内容点击“**是**”按钮后继续执行下一步的安装步骤

4.　出现<用户信息>窗口，在窗口里输入用户名称、公司名称及产品序列号后点击“**下一步**”按钮后继续执行下一步的安装步骤

[注意]
如果不输入正确的产品序列号，产品将自动安装只能使用三十天的评估版本，过三十天后用户将无法继续享受到最新病毒引擎的升级服务以及 V3 VirusBlock 2005 产品的大部分功能

5.　　出现<路径选择> 窗口，V3 VirusBlock 2005 产品的默认路径(C:\Program Files\Ahnlab\V3)，也可以选择其它安装路径，点击“**浏览**”按钮设置其它路径后点击“**下一步**”按钮后继续执行下一步的安装步骤

6.　　出现<文件复制>窗口，确认产品的安装文件夹、名称及安装路径后点击“**下一步**”按钮后继续执行下一步的安装步骤

7.　　出现<安装状态>窗口，此窗口显示产品的安装情况，安装结束后会显示“在线注册”窗口，选择“是，现在进行在线注册用户信息”后会自动连接到相关主页，在主页上填写用户信息就完成了产品的注册

[注意]
如果不输入正确的产品序列号，产品将自动安装只能使用三十天的评估版本，过三十天后无法继续享受到最新病毒引擎的升级服务以及 V3 VirusBlock 2005 产品的大部分功能

8. 完成 V3 VirusBlock 2005 安装后出现<InstallShield 魔法师窗口关闭>的窗口，在窗口里选择将要执行的程序后点击**“完成”**按钮结束本产品的安装

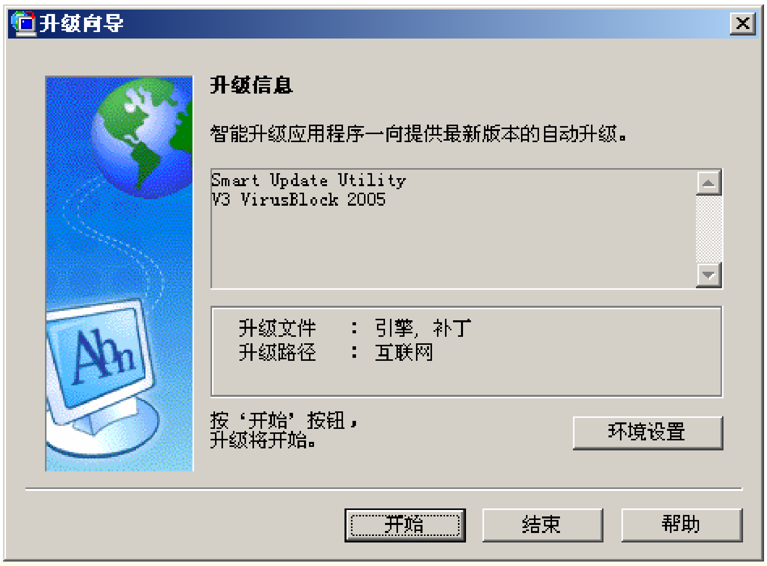
- **智能升级** ： 安装结束后会弹出<智能升级实用工具>窗口，在窗口上点击**“开始”**按钮后产品将自动升级最新的病毒引擎
- **病毒检查** ： 安装魔法师窗口结束后会出现<检查系统>窗口并显示检查结果

[注意]
通过**智能升级**选项升级病毒引擎时用户计算机必须连接到互联网。如果不选择智能升级会弹出<环境设置魔法师 53>窗口

## 启动智能升级

<InstallShield 向导结束>窗口里选择**智能升级**选项后弹出<智能升级实用工具>窗口

1. 在<智能升级实用工具>窗口里点击**“开始”**按钮
→下载最新病毒引擎，分析系统后应用最新病毒引擎




参考
根据系统环境，系统分析需要花一定的时间，请耐心的等待

2. 最新病毒引擎应用于用户系统后会自动弹出升级信息文件‘readme.txt’

3. 确认下载后的最新病毒引擎后关闭 ‘readme.txt’窗口

参考
选择**环境设定**选项可以根据用户需求设置升级环境。详细的设置方法请参考本说明书的‘病毒诊断及杀毒>最新病毒引擎升级 32’ 的部分

## 环境设置魔法师

4. V3 VirusBlock 2005 产品安装及智能升级结束后会弹出<环境设置魔法师>窗口

5. 在弹出的等级设定菜单上选择病毒检查及治疗方式后选择**完成**按钮

## 等级设定

- **最高安全级别 ：** 完全切断病毒的入侵（适合对病毒的安全要求最高的用户）
- **较高安全级别 ：** 切断大部分病毒的入侵（适合对病毒的安全要求较高的用户）
- **一般安全级别 ：** 切断普通病毒的入侵（适合对病毒的安全要求一般的用户）
- **用户自定义安全级别 ：** 用户可以按照自己的需求设置病毒的检查和治疗环境（适合对环境设置有特殊需求的用户）

[注意]
推荐初次使用 V3 VirusBlock 2005 产品的用户可以在“最高安全级别，较高安全级别， 一般安全级别”三个级别当中选择其中的一种级别使用，如果安全级别设定为“最高安全级别”有可能对系统的性能产生一定的影响

## 用户自定义设置

6. 选择**用户自定义**会激活<**下一步**>按钮

7. **点**击<**下一步**>按钮会出现如下表所示的病毒检查及杀毒环境的自定义设置窗口

| | |
|---|---|
| **检查设置** | |
| 没有检查到病毒时自动关闭检查窗口 | 检查病毒结果没有发现病毒时会自动关闭病毒检查窗口 |
| 自动治疗 | 发现病毒后不提醒用户的情况下自动进行治疗 |
| 检查压缩文件 | 检查压缩文件 |
| 检查文件的类型 | • **可执行文件 ：** 检查执行文件，宏文件，脚本文件等能运行病毒的执行的文件<br>• **所有文件 ：** 检查所有类型的文件 |
| **杀毒设置** | |
| 治疗或者删除病毒之前做备份 | 清除或者删除被病毒感染的文件之前备份原文件 |

[注意]
如果在“无法清除病毒的文件”里选择“删除文件”选项时相关文

| | |
|---|---|
| 能治疗的病毒文件 | 选择对能治疗的病毒文件的处理方式<br>• 忽略 ：被病毒感染的文件非常重要时<br>• 治疗<br>• 删除文件 |
| 无法治疗的病毒文件 | 选择对无法治疗的病毒文件的处理方式<br>• 忽略 ：被病毒感染的文件非常重要时<br>• 删除文件 |
| 压缩文件 | 选择对压缩文件的处理方式<br>• 忽略 ：被病毒感染的文件非常重要时<br>**清除病毒后重新压缩(ZIP 文件时)**：检查 ZIP 形式的压缩文件时先解压文件检查/治疗之后重新以 ZIP 形式压缩 |
| 正在运行的文件 | 选择被感染的文件正在运行当中时处理方式<br>• 询问用户后处理：被病毒感染的文件非常重要时<br>• 强制中断运行后治疗病毒<br>• 清除病毒后重新运行文件 |

[注意]
在“治疗设置”里选择“删除”后相关文件会从用户系统里完全被删除掉，被删除的文件会从用户的计算机上完全删除，被删除的文件是无法从回收站或者隔离区里进行恢复，正在运行当中的文件或者加密的文件经处理后虽然文件让在原来的文件夹里面，但是大小已经变为 0 byte

8. 点击**高级…**按钮后在弹出的窗口里可以设置被检查的文件类型及压缩文件类型

| **检查文件的类型** | |
|---|---|
| 所有文件 | 检查所有类型的文件 |
| 执行文件 | 检查执行文件 |
| 宏文件 | 检查宏文件 |
| 脚本文件 | 检查脚本文件 |
| 用户自定义 | 指定检查的扩展名称，选择多个扩展名称时用‘/’分开<br>例） exe/dll/doc |
| **压缩文件** | 检查压缩文件时选择此项 |
| 多重压缩文件 | 检查多重压缩文件时先解压所有层的压缩后检查。选择多重压缩文件的压缩层数 |
| 可执行压缩文件 | 检查 PKLITE， LZEXE， DIET 等可执行压缩文件 |
| 检查一遍 | 不再检查已经检查一遍的压缩文件，更改的压缩文件和新的压缩文件第一次检查一遍后不再检查 |
| 所有压缩文件类型 | 检查所有类型的压缩文件 |
| 选择压缩类型 | 指定检查的压缩文件类型（扩展名称）产品的默认压缩文件类型是‘ace， arj， lzh， rar， zip’ |

9. 点击<**下一步** >按钮后在 V3 VirusBlock 2005 产品功能选项里选择要产品执行的功能，没有选择的选项将不会被执行

| | |
|---|---|
| **系统监控** | 实时监控从用户系统的应用程序里带出来的所有文件 |
| **网络监控** | 实时监控通过网络浏览器下载的所有数据及文件 |
| **聊天程序监控** | 实时监控通过聊天程序下载的所有数据及文件 |
| **启动程序监控** | 实时监控操作系统启动时随机自动启动的注册表，操作系统的服务 |

| | |
|---|---|
| | 程序及各种应用程序 |
| POP3 监控 | 实时监控所有通过邮件客户端程序 POP3 账号接收的邮件,发现带病毒的邮件后及时通知用户 |
| Outlook 检查/监控 | 实时监控通过 MS Outlook 2000 以上的邮件程序接收的邮件，并检查用户邮箱里保存的邮件 |
| **浏览器检查** | MS Internet Explorer(5.0 以上)和资源管理器上显示的 V3 VirusBlock 2005 的工具集和快捷菜单可以非常方便的直接检查用户指定的驱动器，文件夹及文件 |
| **屏幕保护器检查** | 运行屏幕保护器能自动检查按照预先在“检查目录”上设置的区域，如果没有“检查对象”时自动检查用户计算机的系统分区，设置“检查对象”的方法请参考本说明书的‘屏幕保护器’部分 |
| **办公软件保护** | 通过 MS Office 2000 或者 MS Internet Explorer(5.0 以上)用户打开文件, 下载, OLE(Object Linking & Embedding) 时自动检查相关文件 |

# 使用说明书的构成

本使用说明书的内容和桌面 AhnLab 个人防火墙程序受版权以及电脑程序保护法的保护。

## 客户注册

购买桌面 AhnLab 个人防火墙的(以下 AhnLab 个人防火墙)用户，在安装产品后，必须进行在线客户注册。 进行客户注册的用户一年内可以免费享受如下的客户服务。

## 客户服务

- 最新引擎升级: 每周一次定期提供升级，每次有新引擎升级时，可以收到升级向导邮件。
- 各种安全补丁信息: 有紧急病毒扩散时，可以下载单独的安全补丁。
- 提供专用杀毒软件:北京安博士信息安全技术有限公司网页(http://www.ahn.com.cn)的[客户服务]菜单中，直接可以下载。
- 最新紧急病毒警报: 对紧急扩散病毒的警告，告知用户应注意的事项。
- 安全相关信息: 提供各种病毒信息。
- 用户手册以及 FAQ

参考

为了在线进行客户注册，用户的电脑应该与互联网连接。如果电脑没有连接互联网，也可以通过电话或传真进行客户注册。

## 登录更新

购入 AhnLab 个人防火墙之后，超过一年的客户必须购入客户登陆更新产品，才可以继续享有客户服务。如果不购入登陆更新产品，就无法升级最新引擎，也无法诊断和治疗新型病毒。

购入登陆更新产品的方法请参照北京安博士信息安全技术有限公司的网站(http://www.ahn.com.cn)。

参考

AhnLab 个人防火墙的客户服务期限(到期日)可以在北京安博士信息安全技术有限公司网站的[客户服务>产品登陆以及确认]中进行确认。如果希望享受客户服务，就必须先进行客户注册。

## 客户服务联络处

| 北京安博士信息安全技术有限公司的客户服务中心 | |
|---|---|
| 地址 | 北京市海淀区中关村东路 18 号财智大厦 C 座 2005 室<br>邮编:100083 |
| 主页 | http://www.ahn.com.cn |
| E-mail | support@ahn.com.cn<br>V3SOS@ahn.com.cn |
| 电话 | 010-8260-0932(前台) |
| 传真 | 010-8260-0931 |

# 1. 安装方法

安装 AhnLab 个人防火墙之前，先确认需要的配置，仔细说明安装方法。

## 系统配置

安装 AhnLab 个人防火墙，需要具备如下的电脑配置。安装 AhnLab 个人防火墙之前，先确认电脑配置。

### 硬件

| 项目 | 标准配置 | 最低配置 |
|---|---|---|
| OS | Windows 98SP1/98SE/ME/<br>Windows NT Workstation 4.0 SP6<br>Windows 2000 Professional SP4/XP SP1 | |
| CPU | Pentium II 233 以上 | Pentium 133MHz 以上 |
| RAM | 256MByte | 64MByte |
| HDD | 200MB 以上 | 100MB 以上 |
| Resolution | 1024 * 768 | 800 * 600 |
| CD-ROM | 24 倍速以上 | 4 倍速以上 |

注意
AhnLab 个人防火墙不能安装在 Windows 95 系列或 Windows NT/2000 Server/2003 Server。如果要安装 AhnLab 个人防火墙，需要用管理员权限(Administrator)的用户名登录电脑。没有管理员权限的用户名来登录的用户，无法安装和删除 AhnLab 个人防火墙。

### 网络

- LAN: Ethernet 10Mbps
- Fast Ethernet 100Mbps
- Gigabit Ethernet
- WAN: Dial-Up Network, Cable Modem, ADSL

注意
AhnLab 个人防火墙只能安装在作为网络终端点使用的客户端电脑。包括多个 LAN 卡， 安装 WinGate、SyGate 等路由程序，支持互联网连接共享的电脑，不能安装 AhnLab 个人防火墙。

最新引擎升级

首次执行 AhnLab 个人防火墙的用户，必须先进行最新版本引擎的升级。为了检测和治疗每周新发现的新型病毒，必须定期升级最新引擎。

注意
如果要通过升级向导，升级最新版本的引擎，用户电脑就必须连接互联网。

## 升级向导

选择下列方法中的一种，执行 AhnLab 个人防火墙。

- 双击桌面的 AhnLab 个人防火墙快速连接图标。
- 任务栏中双击 AhnLab 个人防火墙提示图标。
- 右击任务栏中 AhnLab 个人防火墙提示图标，选择**打开**。

选择下列方法中的一种，执行升级向导功能，升级最新引擎。

- 工具栏中点击**升级**。
- 位于上方的菜单条中选择**文件(F)>升级向导(U)**。
- 任务栏中右击 AhnLab 个人防火墙提示图标，选择**升级向导**。
- Windows 资源管理器或 MS Internet Explorer(5.0 以上)的 V3 工具栏中，选择**升级向导**。

出现<升级向导功能>窗，点击**开始**，开始升级。

分析要升级的最新引擎文件，将用户系统中的引擎升级为最新版本。

参考
根据不同系统环境，系统分析需要几分钟，所有作业结束为止，请稍等。

升级完成后，出现升级信息文件 readme.txt。确认升级后的最新引擎信息后，关闭 readme.txt。

参考
AhnLab 个人防火墙的开始菜单中，点击**查看更多引擎升级内容**，就可以重新确认升级信息文件 readme.txt 的内容。

注意
执行中的文件被更新后，必须重新开始系统。**黑客工具的探测以及截断**
介绍利用 AhnLab 个人防火墙实时截断，通过网络或互联网入侵的蠕虫病毒、黑客工具以及攻击性包入侵的方法。使用 AhnLab 个人防火墙共享规则，就可以实时控制对共享文件的访问。

# 执行方法

**基本设置**
设置 AhnLab 个人防火墙的使用所需的基本项目。

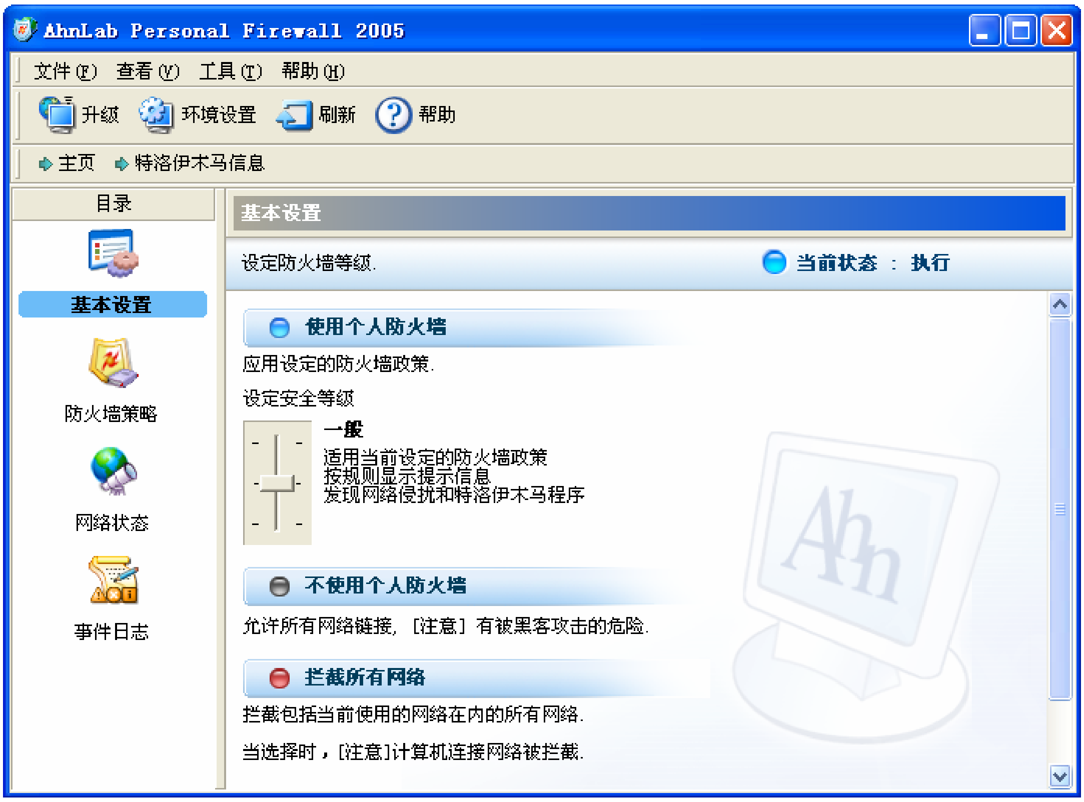
**防火墙策略**
使用 AhnLab 个人防火墙，可以编辑和选择适用到用户系统的个人防火墙策略。

**网络状态**
通过 AhnLab 个人防火墙适用到系统的防火墙策略，截断或允许的网络状态。

**事件记录**
按日期显示，使用 AhnLab 个人防火墙所执行的所有工作内容。

# 基本设置

选择 AhnLab 个人防火墙的基本设置菜单，就出现如下的工作窗。使用各种菜单，选择是否要执行防火墙策略。




☑ 参考个人防火墙(Personal Firewall)
为了保护单一互联网连接电脑免遭外部入侵而使用的软件应用程序。像 DSL（digital subcriber line)或线缆调制解调器等长时间保持连接状态的用户相比，使用 IP 地址连接互联网的电脑容易遭到黑客攻击，因此个人防火墙程序是非常必要的。与防病毒应用程序相比，个人防火墙修补链接阶层和网络阶层的缺陷，防止黑客通过互联网非法访问电脑。而且，能保护系统数据的调制，还向用户提示外部入侵。

☑ 参考
右击任务栏的 AhnLab 个人防火墙提示图标，可以便捷地设置基本设置。

一般建议，选择**执行防火墙**，实时探测和截断访问用户系统的黑客工具。

### 1.2.1. 执行防火墙

APF 提供的基本防火墙策略适用到用户电脑。选择要执行的防火墙策略安全水平。

**高**

- 当前启用中的防火墙战略，适用到用户系统，探测网络入侵。
- 发现网络连接(TCP)后，根据目前启用中的防火墙战略，允许或截断，然后通过任务栏的提示信息，向用户显示其结果。.
- 特洛伊木马程序或网络入侵中注册的程序，就立即截断。

☑ 参考

如果防火墙执行的**安全水平设置**中选择**高**，就会每次发现网络访问(TCP)时，都会出现提示信息。如果不想看到提示信息，就将安全水平改为**普通**。

### 一般

- 当前启用中的防火墙战略，适用到用户系统，探测网络入侵。
- 发现网络连接(TCP)后，根据目前启用中的防火墙战略，允许或截断，但是不会通过提示信息告诉用户。
- 特洛伊木马程序或网络入侵中注册的程序，就立即截断。

### 低

- 不会将当前启用中的防火墙战略适用到用户系统。就是说，允许所有网络访问。
- 发现网络访问(TCP)时，无条件允许访问。
- 如果特洛伊木马程序或网络入侵上注册的程序尝试网络访问时，就立即截断。

注意

如果系统保护水平设为**低**，就会除了**特洛伊木马程序**或**网络入侵上注册**的程序之外，所有网络访问都被允许。注册的个人信息也不能得到保护。个人信息保护相关的详细说明清参照[5.4 个人信息]。

参考

TCP(Transmission Control Protocol):两个主机之间的数据传送，保证可靠性的
通信协议。特洛伊木马(Trojan): 指病毒名称中包含 Trojan 的程序，常住系统内存领域，妨害用户电脑执行工作。特洛伊木马程序是故意编写的程序，与臭虫(Bug)程序不同，并且与电脑病毒不同，不会将自己复制到其他文件。

## 1.2.2. 不执行防火墙

不会将防火墙策略适用到用户系统。因此，所有网络访问都被允许。**特洛伊木马**程序或**网络入侵上注册**的程序也都被允许。

注意

如果选择**不执行防火墙**，所有网络访问都将被允许。特洛伊木马程序、恶性程序以及黑客程序入侵到用户系统，有可能出现错误。并且，无法保护已经注册的个人信息。个人信息保护相关的详细说明，请参照[5.4 个人信息]。

## 1.2.3. 截断所有网络

与防火墙策略无关，切断当前用户正在访问中的所有网络连接。建议在网络使用量急剧增加等黑客入侵的可能性较高的情形下，作为应急措施使用。

注意

如果选择，防火墙的执行中截断所有网络，传送中的邮件就会完成传送。如果突然截断使用中的网络，就有可能导致系统错误，需谨慎。

# 应用程序的互联网访问控制

如果在基本设置中选择，**执行防火墙**时，根据基本防火墙策略，实时探测用户系统。如果发现尝试互联网访问的应用程序时，就显示如下的<设置应用程序的因特网访问>。

详细的安装信息请参照安装光盘里面的产品说明书